REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

The specification has been placed in a more traditional U.S. format by adding headings.

Claims 1-12 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter.

Reconsideration of this rejection is respectfully requested.

Independent claim 1 calls for "means for selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware". Independent claim 7 includes a corresponding limitation of "selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware".

Applicant submits that these claims and the claims that depend therefrom relate to statutory subject matter because these claim limitations do in fact specify a practical application, not just an abstract idea. The result of these limitations is a determination of whether or not the file contains, or is likely to contain, malware. This determination is a tangible result that has real world value and provides an immediate benefit. This is because the determination allows the system (or user) to decide on how the file is subsequently handled. This is very much a real world benefit. By way of example without limitation, the claimed system/method may be implemented and the determination used to control whether emails and other documents are passed through the system.

Claims 1 and 7 were rejected under 35 U.S.C. Section 102(a) as allegedly being "anticipated" by Cowie (GB 2378015). By the above amendments, the subject matter of claim 2 has been incorporated into claim 1 and the subject matter of claim 8 has been incorporated into claim 7. Consequently, the rejection of claims 1 and 7 as being anticipated by Cowie is believed to be moot.

With respect to claims 2 and 8, these claims (along with claims 3-6 and 9-12) were rejected under 35 U.S.C. Section 103(a) as allegedly being "obvious" over Cowie in view of Roberts (U.S. Patent Application Publication 2004/0088570). Applicants traverse this rejection for the reasons set forth below.

The office action contends that (1) Cowie discloses all the limitations of claim 1 as previously presented; (2) Roberts discloses the limitation of claim 2 as previously presented; and (3) it would have been obvious to combine the references. Applicant submits that no prima facie case of obviousness can be established in respect of claim 1 as now amended, because the two references do not in fact disclose all the limitations of amended claim 1, whereby no combination of the two references can result in the subject matter of amended claim 1. The reasons for this are as follows.

Cowie discloses a method and system for scanning a packed file to determine whether or not it contains malware. Even assuming for the sake of argument that Cowie's disclosure of using of three fingerprints derived from characteristics of the resource data of a file is viewed as selectively subjecting the file to a heuristic procedure to determine whether or not it contains, or is likely to contain, malware as recited in claims 1 and 7, Applicant submits that Cowie does not disclose the feature a) or feature c) of these amended claims.

Feature a) calls for generating data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file. Cowie does not disclose such a feature because there is no generation of data which characterises the identity of a file. The office action alleges that this limitation can be found on page 2, lines 30-31 and page 6, lines 10-31 of Cowie. Applicants disagree. These passages of Cowie both disclose generation of a fingerprint for file known to be a Trojan. This generation is described in more detail on page 9, lines 1 to 22 and in Fig. 5 of Cowie. However, such a fingerprint does not "characterize its [i.e. the file's] identity" as required by claims 1 and 7. To the contrary, such a fingerprint is a heuristic. That is to say, if the fingerprint is present in a file under examination, there is a high probability of the file under examination being the file from which the fingerprint is generated, but the identity of the file is not determined. There remains a probability that the file under examination has a different identity but by chance has the fingerprint within its data.

Feature c) calls for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected and for controlling feature b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or

not subject to processing by the feature b) at all. Cowie does not disclose such a feature. In Cowie, there is no determination of whether the file can be regarded as safe in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected. As a result, Cowie also fails to disclose control of feature b) on the basis of such a determination.

The office action contends that feature c) as previously presented is disclosed in Cowie on page 10, lines 6-9 and page 10, lines 14-15. Applicant traverses this contention. These passages relate to the scanning process illustrated in Figure 5. In this process, fingerprints generated from the file under examination (in step 36) are compared (in step 42) with fingerprints previously generated from known Trojans (using the process of Fig. 5) and stored in a database. The comparison against all fingerprints in the database is performed by looping around steps 40 to 48. If there is a match, the process comes out of the loop to step 46.

It follows that all files under examination in Cowie are subject to the same thoroughness of scanning because they are compared against all the fingerprints stored in the database. One could argue that in the event of detecting a Trojan resulting in the process of Figure 5 coming out of the loop to step 46, there is less processing. However this is entirely different from feature c), because it only occurs when a Trojan has been detected. In other words, in Cowie, no subsequent processing is performed when a Trojan is detected, i.e. when the file is not safe, in contrast to feature c) which requires that less thorough processing is performed when the file is safe.

In any event, Cowie does not disclose the feature c) limitation of determining whether the file can be regarded as safe "in dependence on factors including the length of time for which the database indicates that the file has been known without malware containing instances of it being detected".

The office action further contends that the claim 2 and 8 features (now incorporated into claims 1 and 7, respectively) are disclosed on paragraph 34, lines 6-8 and paragraph 37, lines 1-6 of Roberts. Applicant traverses this contention.

Roberts discloses a system implemented in a firewall in which web pages identified by links in documents (e.g. emails or files) are preemptively scanned for malware. Thus, when the user subsequently clicks on the link, the webpage can be retrieved without scanning it again. This avoids a delay associated with scanning the webpage after the user clicks on the link.

Paragraph 34, lines 6-8 of Roberts discloses that, in the database of addresses which have been preemptively scanned and found safe, a date is stored. The storage of this date does not meet any requirement of feature c).

Paragraph 37, lines 1-6 of Roberts discloses that, when the user clicks a link for a web page which was preemptively scanned and found to be safe, prior to retrieval, a check is performed on whether the web page has changed since it was scanned. Such a check does not meet any requirement of feature c).

Thus Roberts does not in fact disclose any technique which considers the factor of "the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected" which is required to be considered by feature c). Indeed, Roberts does not disclose any part of feature c).

Therefore feature c) is not disclosed (or even suggested) by either Cowie or Roberts, and consequently no combination of features from Cowie and Roberts can result in all the claim limitations of claims 1 and 7.

Claims 3-6 depend from claim 1 and claims 9-12 depend from claim 7. These claims are believed to distinguish from the proposed combination of Cowie and Roberts at least because of these dependencies.

New claim 13 has been added. This claim is believed to distinguish from the applied references for reasons similar to those advanced above with respect to claims 1 and 7.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Michael J. Shea
Reg. No. 34,725

MJS:dbp
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100